CYBER OFFENDING IN NIGERIA: AN OVERVIEW

[1]Soyombo Luke; [2]Attoh Franca

Abstract
This paper provides an overview of cyber-offending in Nigeria. It looks at the state of research and theory on cyber-offending. It shows the gap in knowledge and justification for empirical research on cyber-offending from correction's perspective i.e. seeking empirical insights from correctional centres in Nigeria. The paper uses scholarly papers and Economic and Financial Crimes Commission's Report on Cyber-Offending. Theoretically, this paper is anchored on Space Transition Theory (STT), Routine Activity Theory and Social Learning theory. It argues that cyber-offending in Nigerian context is largely characterised by cyber-enabled crimes that are motivated by economic/financial gains. Essentially, cyber-offending in Nigerian context can be succinctly conceptualised as the use of computer/internet to perpetrate fraud. It recommends that the Cyber Act of 2015 should be properly implemented, and issues of poverty, inequality and cumulative deprivation should be adequately addressed by the Nigerian state.
Keywords: Cyber-offending, cyber-enabled crime, cyber-dependent crime, cyber-fraud.

Introduction

Cyber crime is a serious problem that plagues the twenty-first century world. With a global population of 7,875,765,587 (United Nations Population Fund, 2021) and5,168,780,607of internet users in the world (Internet World Stat, 2021), the globalization of crime, deviance and terror in the cyberspace makes the phenomenon of cyber crime more complicated. Kranenbarg et al (2018) averred that cyber-crimes provide the sharpest contrast to traditional crimes, as they completely take place in the digital or cyber space. The World Economic Forum's report Globalization 4.0 shows that more organisations are conducting business online (Davos, 2019). Okemuyiwa & Ibraheem (2019) assert that cyber criminality presents unique problems of investigation for prosecution due to the global nature of the internet. The internet, computers and cell phones have revolutionised every aspect of the human life (Holt & Bosssler, 2016). These technological revolution and advancement have also created series of opportunities for offenders to commit various forms of cyber crime (Bossler & Berenblum, 2019. Put succinctly, cybercrime is a serious threat that faces the contemporary world as the cost of cyber crime globally increased from $445 billion in 2014 to $600 billion in 2017 (Lau, 2018). This is more than the GDP of South Africa ($349.6 billion) and that of Nigeria ($405 billion), the continent's largest economies (Africa Cyber Security, 2019).It was projected that in 2020, global security spending would reach $170 billion, a 126% increase from $75 billion in 2015 (Umaru, 2019). The Internet Crime control Centre (IC3) report revealed that in 2020, a record number of 791,790 complaints of cybercrimes were received with reported losses exceeding $4.1 billion. This shows a 69% increase in total complaints from 2019. Business E-mail compromise (BEC) continued to be the costliest accounting for 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent accounting for 241,342 complaints with adjusted losses of $54 million while the number of ransom ware incidents also continue to rise, with 2,474 incidents reported in 2020 (Internet Crime Control Centre, 2021).

In Africa, it was projected that a billion people would be able to access the internet by 2020

(Kshetri, 2019). The Internet World Stats (2021) which provides the internet usage and world population statistics estimates said that there are 594,008,009 internet users with 43.2% penetration in Africa, representing 11.5% of the population of internet users across the globe exposing the world to more vulnerabilities in terms of cyber-crime.

In a broad sense, cybercrimes can be classified into different categories, including cyber-trespass (e.g., unauthorized system access), cyber-deception/theft (e.g., identity theft, online fraud, digital piracy), cyberporn/ obscenity (e.g., child sexual exploitation materials), and cyber-violence (e.g., cyberstalking; cyber terrorism) (Holt, Bossler & -Spellar, 2018).

In Nigeria, various types of cybercrimes are committed daily, and they include cyber fraud, identity theft, hacking, phishing, spamming, Automated Teller Machine Spoofing, digital piracy etc. According to estimates, cyber crime costs the Nigerian economy the sum of $ 500 million per annum (Umaru,2019).

In real and concrete terms, cyber criminology is an evolving epistemic area in criminology and criminal justice system and should be noted that there is dearth of research focusing on the correlates of cyber offending from a correction's perspective i.e. seeking empirical insights from correctional centres. Though some studies have been conducted on cyber crime globally and in Nigeria, but the focus has largely been on cyber crime victimisation (e.g., [Ndubueze,2013; Ndubueze, Igbo & Okoye, 2013; Radda & Ndubueze, 2013; Mambe, Magaji & Damagun, 2014 etc.]). There is an epistemic lacuna as regardscyber-offending, especially the socio-economic and demographic correlates of cyber-offending in Nigeria from a correction's perspective.There is concrete need to examine the characteristics of offenders to better understand the nature, causes and dynamics of cyber crime in Nigeria as it poses a serious threat to the social and economic wellbeing of the country.

In recent years, cybercrime is becoming increasingly one of the ubiquitous problems of developed and developing countries including Nigeria. Since 2009, nation states have signed 33 multilateral as well as 30 bilateral agreements on global action against cybercrime (Daultrey, 2017). Also, global cyber security market is worth an estimated $120 billion (Daultrey, 2017). These underscore the gravity of the menace of cybercrime and the global challenges it poses.Cybercrime has attracted enormous academic attention over the years. However, in Nigeria, not so much comprehensive empirical research has been conducted in the epistemic area of cyber-offending unlike cyber-victimisation. To this significant end, this paper seeks to look at research on cyber-offending from an empirical point of view.

Operational Definition of Terms

This section of the paper operationalises/ conceptualises terms such as cybercrime, cyber-offending, cyber-dependent crime, cyber-enabled crime, socio-economic and demographic variables, and correctional centres.

Cybercrimes: These are offences that are committed in the cyberspace through a computer and computer networks. Essentially, it is the use of computer and internet to commit fraud.

Cyber-offending: This is constructed in this study as a variable that indicates conviction, sentencing and incarceration due to cybercrime

Cyber-dependent crimes: They are offences that can only be committed by using a computer, computer networks, other forms of Information and Communication Technology (ICT).

Cyber-enabled crimes: These are traditional crimes in which a computer and computer networks are used in the commission of the crime.

Correctional centres: These are places where offenders of cybercrime are incarcerated and rehabilitated.

Review of Extant Literature

The literature review covers scholarly research on

cybercrime and cyber-offending. Specifically, in the empirical review, it looks at grey areas and gap in knowledge in respect to socio-economic and demographic correlates of cyber-offending.

Cybercrime and Cyber-offending

Daultrey (2017) construe cybercrime as crimes in which ICT devices are both the tool and target. Cyber dependent crimes are crimes that are a direct result of computer technology (McGuire & Dowling as cited in Kranenburg et al., 2018). According to (Kranenburg et al., 2018), cybercrimes are crimes that cannot be perpetrated without the use of Information Technology Systems (ITS) and was not in existence before the advent of IT-systems. Examples of cyber dependent crimes are malicious hacking of computer, email accounts, websites, or online profiles, using malware and blocking access to websites (e.g. by flooding a web server with unwanted traffic, a Distributed Denial of Service (DDoS) attack). Kranenburg et al (2018) stressed that cyber-dependent crimes present a stark contrast to traditional crimes because they occur in the digital realm. By way of contrast, traditional crimes in which Information technology systems are used in commission of crimes are cyber-enabled crimes such as online fraud, online theft and online harassment(McGuire & Dowling as cited in Kranenburg et al., 2018).

From the perspective of an investigator, analysis of a cybercrime generally has three phases: (i) detection; (ii) attribution; and (iii) analysis. Essentially, for law enforcement agencies to embark upon a formal investigation, police must first determine which criminal law has been violated (Grabosky as cited in Daultrey, 2017).

Detection

Cybercrimes are perpetrated in one or more of five patterns: (i) one-to-one (a single attacker against a single target); (ii) one-tomany;(iii) many-to-many; (iv) many-to-one; (v) multi-stage hybrid attack (a combination of methods) (Johnson as cited in Daultey, 2017). These patterns have signatures and an investigator will typically search for 'indicators of compromise' (IOC) e.g. IP addresses, URLs of C2Servers, malware hash functions (Daultry, 2017).

Attribution

Establishing the perpetrator of a crime is as old as the art of crime itself, at the core of crime-fighting and the legal response. Attribution could be generally divided into tactical and operational questions (investigating how the crime was committed, identifying what the target was, who the perpetrator(s) were, the scale and timeline) and strategic questions (understanding rationale and significance of the attack, figuring out appropriate response, mitigating similar future attacks) (Rid & Buchman as cited in Daultrey 2017).

Analysis

In terms of analysis, law enforcement agencies use similar techniques in the cyberspace as in the terrestrial space. As deemed necessary, they may carry out, run search and surveillance operations, conduct forensic examinations, seek, and share information with other agencies. Essentially, law enforcement agencies ought to obtain the necessary warrants, avoid contaminating evidence, ensure the investigation is conducted lawfully and ultimately avoid bias in their findings and conclusions. (Digital shadows as cited in Daultrey, 2017).

In his work on taxonomy of cybercrime, Ibrahim (2016) presented a binary (dual) model of cybercrime and a tripartite cybercrime framework (TCF).

A binary (dual) model of cybercrime

Cyber Enabled Crimes/People-centric	**Cyber Dependent Crimes/Techno-centric**
• Fraudulent Sales Online (e.g.) E-bay • Cyber-bullying • Online romance scam • Cyber Stalking • E-commerce fraud • Consumer Scams • Advance Fee Fraud	• Hacking • Distributed Denial of Service (DDoS) • Phishing • Malware (Virus, Worms, Trojan) • Cyber Vandalism

Source: (Ibrahim, 2016)

According to Ibrahim, cybercrime comprises a

wide range of online or digital crimes. Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other forms of Information and Communication Technology such as creation or/ and distribution of malware or viruses. While cyber enabled crime can still be perpetrated without the use of Information and Communication Technology such as cyber fraud. According to Yazdanifard et al.(as cited in Ibrahim, 2016), cybercrime in the realm of cyberspace may involve a few nations and actors and have an impact on them concurrently. Yar & Jewkes (as cited in Ibrahim, 2016) asserted that cybercrime is usually committed on a global level. For instance, if an individual creates a computer viruses or malwares in Russia whilst someone in Nigeria rents it to send credit scam emails and a third-party transfers funds using illegally acquired data in United States, (Wall as cited in Ibrahim, 2016), all three individuals are culpable in different strands of cybercrime. While the three individuals are motivated by monetary gains, they are at the same time engaged in cyberspace in different degrees. The individual who created the virus/malware committed a cyber-dependent crime while the other two actors committed cyber-enabled crime (Ibrahim, 2016).

Tripartite Cybercrime Framework (TCF)

Socio-economic	Pyscho-social	Geo-political
Hackers and Crackers	Hackers and Crackers	Hackers & Hacktivist
Cyber fraud	Child pornography	Cyber spies
Cyber embezzlement	Cyber stalking	Cyber espionage
Cyber piracy	Cyber bullying	Cyber terrorism
Cyber blackmail	Revenge porn	Cyber vandalism
Romance scam	Cyber rape	Cyber assault
Online drug trafficking	Cyber hate speech	Cyber hate speech
Cyber prostitution	Cyber extortion	Cyber riot
Cyber extortion	Obscenity	Cyber sabotage
Illegal online gambling	Cyber prostitution	Cyber colonialism
Cyber trespass	Cyber trespass	Cyber rebellion
Cyber terrorism	Cyber homicide	
	Cyberterrorism	

Source: Ibrahim (2016)

Ibrahim (2016) proposes that cybercrimes are motivated in three different ways, i.e., socioeconomic, psychosocial, and geopolitical. He acknowledges that certain types of cybercrimes fit into two or more motivational categories. However, there is a degree of overlap between the categories as the primary motivation behind the action is the basic tool to differentiate between types of cyber crimes. For instance, while cyber fraud is under socioeconomic cybercrime umbrella, revenge porn is under the category of psychological cyber crime. Fundamentally, socio-economic cybercrimes are construed as economically or financially motivated crimes that are computer or/and internet-mediated such as online fraud, romance scam, e-embezzlement and the offender usually has a direct contact with the victim. In contrast, psycho-social cybercrimes ate offences that are fundamentally driven such as cyber stalking, cyber harassment, cyber rape to mention but a few. Perpetrators of psycho-social cybercrimes focus primarily on inflicting psychological distress on their victims (Ibrahim, 2016). However, it is valid to note that financial loss due to socioeconomic cybercrime such as cyber crime may manifest psychologically as distress (Lazarus, 2006).

According to Ibrahim (2016), geopolitical cybercrimes are e-crimes that involve agents of statecraft or/ and industrial representatives such as cyber espionage. However, geopolitical cybercrimes constitute some elements of socioeconomic and psychosocial cybercrimes. The actions of some perpetrators of geopolitical cybercrimes could have economic, psychosocial, and geopolitical consequences on a person or group of persons. Albeit as regard the nexus of interaction between victims and perpetrators, whilst socioeconomic and psychosocial cybercrimes are primarily orchestrated and perpetrated on individual levels, geopolitical cybercrimes are fundamentally actions of state agent, groups of individuals against other groups, nations or industrial entities acting on behalf of more complex statecraft or vested interests. Furthermore, agents of statecraft that perpetrate geopolitical crimes are seldom considered as 'criminals' in their hometown. The assumption underlying this is that they represent authority rather than subversion. Consequently, it is the nation they represent that is considered as criminal unlike individual sub-cultural offenders such as the Nigerian cybercriminals (Ibrahim, 2016).

Criminalisation of Cybercrime in Nigeria

Several laws have been enacted in different countries globally and Africa to criminalise cybercrime. In Nigeria, Cybercrime Act (2015) was promulgated to criminalise cybercrimes and related offences. Adesina (2017) opined that enacting a law is one of the major steps in curbing cybercrime. According to Ndubueze (2020), The Council of Europe/Project Cybercrime@Octopus (2016, p. 5) specifically evaluated the criminal law provisions on cybercrime and electronic evidence in the54 countries of Africa and reports that as of April 2016, 11 countries had basic substantive and procedural law provisions enacted in Africa. These countries are Bostwana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda, and Zambia. Also, 12 countries had substantive and procedural law provisions partially in place. These nation-states include Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia, and Zimbabwe. The report also stated that majority of African states (30) had no specific legal provisions on cybercrime and electronic evidence in place. It was further reported that draft laws or amendments to existing legislation reportedly had been prepared in at least 15 counties including Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe.

In furtherance, United Nations Conference on Trade and Development (2019)reports 28 (52%) of countries in Africa have cybercrime legislation, 11 (20%) have draft cybercrime legislation, and 15 (28%)do not have cybercrime legislation (Ndubueze, 2019).

The Cybercrimes Act of 2015

Essentially, The Cybercrimes Act 2015 is the first legislation in Nigeria that deals specifically with cybercrimes and cyber security(Adesina, 2017). Some of the provisions of the Act include:

a) The act provides the president the power to designate certain computer systems, networks, and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure, and to implement procedures, guidelines, and conduct audits in furtherance of that. Examples of systems, which could be designated as such, include transport, communication, banking etc.

b) The act recommends the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that result in the death of an individual (amongst other punishments for lesser crimes).

c) Perpetrators of Hacking, if found guilty, of unlawfully accessing a computer system or network, are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages or accessing and using data stored on computer systems.

d) The act provides for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment.

e) The act explicitly makes provision for child pornography offences, with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.

f) The act prohibits Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to

a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

g) The act outlaws cyber-squatting, which is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.

h) The act frowns at the distribution of racist and xenophobic material to the public through a computer system or network (e.g., Facebook and Twitter). Furthermore, it prohibits the use of threats of violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10million or to both fine and imprisonment.

I) The act makes it mandatory that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy and shall take appropriate measures to safeguard the confidentiality of the data retained, processed, or retrieved.

j) The act specifically allows for the interception of electronic communication, by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings (Cybercrimes Act, 2015).

Forms of Cybercrime

Essentially, there are over thirty types of cybercrimes identifies in existing literature (Ibrahim, 2016). Justice is done to some of the common cybercrimes (cyber-dependent and cyber-enabled) below.

S/N	Form	Narrative
1	Hacking	Involves breaking into a pers on's computer to compromise information. This is often perpetrated from a remote location and takes advantage of loopness in the victim's computer programme. Hackers can also monitor what the victim does on the computer and can also import files such as pa ssword, credit card information, company data, business plans etc.
2	Cyber theft	The use of computer to steal electronic information falls under this category. Herein, hackers break into the system of banks and transfer money to a third-party account. Cyber theft is one of the most common forms of cybercrime as it promises a large sum of money for experienced cyber criminals. However, individuals are not exempted from this form of attack as cyber criminals access a victim's banking information to siphon mo ney or buy expensive items in the victim's name.
3	Cyber stalking	This refers to the subjection of an individual to harassment over the internet. It often involves sending life threatening messages to the victim.
4	Software, virus and worms	Cyber criminals also create and spread internet -based malicious software known as viruses and worms to disrupt a victim's computer network and gain access to sensitive information or to cause damage to the system. Viruses and worms are capable of damaging system s and are often attached to some other programme or documents through which it enters the computer.
5	Cyber terrorism	This is a large-scale disruption of computer networks through viruses to spread fear and panic or to destroy computer networks mostly for political and ideological reasons.
6	Cyber espionage	This refers to the illegal use of a computer to steal state secrets, spy on another g overnment, or gain information about a government's clandestine operation.
7	Child soliciting and Abuse	Cybercriminals are known to often solicit for, and abuse minors in chat rooms for child pornography
8	Intellectual theft	This occurs when a person vio lates copyrights or downloads unlicensed intellectual properties such as movies, music, games, and software on the internet. Disturbingly, some websites encourage software piracy.
9	Phishing, website cloning and Spamming	Cybercriminals are also known as spam emails by sending mass emails to promote and advertise fictitious products and websites in a bid to promote their business or products. These criminals may clone a well-known website to deceive their victims who often end up imputing credit card detai ls and other personal information which the criminals later use to commit credit card fraud. Moreover, cyber criminals are also in the habit of posing as a known dignitary or celebrity to lure their victims with business transactions. This is a very common cybercrime among Nigerians.
10	Business Email Compromise (BEC) and Romance Fraud	BEC, another common cybercrime in Nigeria is the act of sending an email from spoofed or com[promised account to the victim's company's financial institution requesting a wi re transfer. Once the transfer is sent, the payment details are intercepted by the cybercriminals and changed. The fraud operations are often driven by syndicated based in Nigeria, which may target a U.S. based business and then move stolen funds to Mexico, Ireland, or China. Nigerian cyber criminals are also known to pretend to be opposite gender of their victim in a bid to facilitate romance and gain the trust of the victim before attacking.

Source: African Cyber Security (2019)

2.2.4 Cost of Cybercrime

Cybercrime cost in Africa by Industry

Bank and Financial Services	23 per cent
Government	19 per cent
e-Commerce	16 per cent
Mobile-based transactions	13 per cent
Telecommunications	11 per cent
Other sectors/industries	18 per cent

Source: Signe & Signe (2018)

Cost of cybercrime: Nigeria in comparison to other counties in Africa

	Population (2017 Est)	GDP (2017) in USD	Penetration % population (2017)	Estimated cost of cybercrime (2017)	Estimated No of certified professionals (2017)
Africa	1,300,000,000	$3.3T	35%	$3.5B	10,000
Nigeria	195,875,237	$405B	50%	$649M	1,800
Kenya	50,590,879	$70.5B	85%	$210M	1,600
Tanzania	59,091,392	$47B	39%	$99M	300
Uganda	74,270,563	$24	43%	$67M	350
Ghana	29,463,643	$43B	34%	$54M	500
Namibia	2,587,801	$11B	31%	*	75
Botswana	2,333,201	$15.6B	40%	*	60
Lesotho	2,263,010	$2.3B	25%	*	30
Mauritius	1,263,315	$12.2B	63%	*	125

Source: Africa Security Report (2019)

Empirical Review

Age and Cyber-offending

There is extant literature on age and cyber offending outside Nigeria (Hadzhidimora & Payne, 2019; Harbinson & Selzer, 2019; UNODC, 2013). In their study that explores the characteristics of cyber offenders prosecuted in the United States, Hadzhidimora & Payne (2019) found out that the average age of the offenders in their study is slightly higher than others who do not focus exclusively on international offenders. In their study, the minimum age of cyber offenders is 19 years, and the maximum is 73. The average age of cyber offenders is 34.79. In a study conducted in the United States by Harbinson & Selzer (2019), it was discovered that average of cyber offenders on federal supervision was 38.2 %. This is in sharp contrast to studies which indicate that the stereotypical perpetrator of a cybercrime is 12-28 years old (Rogers as cited in Hadzhidimora & Payne, 2019).According to the report of UNODC (2013), the demographic nature of cyber offenders in Asia mirrors traditional crime because young males are the majority offenders, although the age profile is increasingly showing older (male) individuals, particularly concerning child pornography offences.

Gender and Cyber-offending

According to studies on gender and cyber offending, the stereotypical perpetrator of a cybercrime is male (Rogers, 2011). In a study carried out by Hadzhimora& Payne (2019), the analysis shows that cybercrime offenders on federal supervision were more often male. Their study further revealed that only 6 per cent or 13 out of 225 are females. By way of contrast, a study also conducted in the United States by Harbinson & Selzer (2019) unexpectedly found out high percentage of female offenders (21.8%).

Marital Status and Cyber-offending

In their study in Netherlands, Kranenburg et al (2018) found out that when an individual is cohabiting, that individual is less likely to commit a crime than when those individuals live alone. The partner in a household seems to be the most important source of informal social control, especially for cyber offending. Furthermore, their study revealed that an individual is less likely to commit cybercrime in years in which that individual shares a household with a partner, with or without children, than in other years. In the study, 32.8%, 5.0%, 38.3%, 11.8%, 3.7% and .2% account for single, cohabiting, married, divorced, separated, and widowed respectively.

Educational Attainment and Cyber-offending

Karenburg et al(2018) in their study in Netherlands did not find a strong and statistically significant protective effect of education on cyber offending. In the complete offender population data used in their study, they found that education increases the odds that an individual commits a cybercrime. In other words, they discovered that education is not statistically significantly related to cyber offending. However, the study carried out by Harbinson & Selzer (2019) in United States revealed that there is a statistically significant relationship between educational attainment and cyber offending.

Employment Status and Cyber-offending

In their study conducted in the Netherlands, Kranenburg et al (2018) did notfind a strong and statistically significant protective effect of employment on cyber offending. In other words, employment increases the odds that an individual commitsa crime. According to the authors, employment is not statistically sign8ficantly related to cyber offending. By way of contrast, the study of Harbinson & Selzer (2018) found that there is a statistically significant relationship between employment status and cyber offending.

Existing Gap in Knowledge

From the empirical review, it is obvious that there is paucity/dearth of research on the socio-economic and demographic correlates of cyber-offending in Nigeria from a correction's perspective i.e. seeking empirical insights from correction centres in Nigeria through individuals who have been convicted, sentenced and incarcerated. Most of the studies in this epistemic area were conducted in United States, Netherlands etc.

Theoretical Underpinnings

Theoretically, this paper is anchored on Space Transition Theory (STT), Routine Activity Theory, Social Learning theory, Anomie Theory and Marxist Theory of the State.

Space Learning Theory

Prof. K. Jaishankar (2008) propounded the Space Transition Theory (STT) essentially, he is reputed as the founding father of cyber criminology having academically coined the term in 2007. The theory proposes the following key assumptions as explanations to criminal behaviour in the cyberspace:

a) Persons with repressed criminal behaviour in the physical space have a propensity to commit crime in cyberspace, which otherwise they would not commit in the physical space due to their status and position.
b) Identity Flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provide choice to commit crime.
c) Criminal behaviour of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to the cyberspace as well.
d) Intermittent venture of offenders in the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape
e) [i] Strangers are likely to unite in cyberspace to commit crime in physical space, [ii] Associates of physical space are likely to unite to commit crime in cyberspace.
f) Persons from closed society are more likely to commit cybercrime than persons from open society.
g) The conflict of norms and values of physical space with norms and values of cyberspace may lead to cybercrime.

Routine Activity Theory

According to (Kigerl as cited in UNODC, 2013), Routine Activity Theory provides insight into underlying drivers of cybercrime. The theory proposes that crime increases upon the convergence of (a) a motivated offender, (b) a suitable target, and (c) the absence of a capable guardian. In the case of cybercrime, large numbers of suitable targets may emerge through increasing time spent online, and the use of online services such as banking, shopping and file sharing, making users prone to phishing attacks and fraud.

The theory claims that cybercrimes are more likely to be committed by motivated offenders who are suitable targets in the absence of capable guardians. Furthermore, routine activities of perpetrators, as well as those of potential victims and other actors result in opportunities for committing and preventing cybercrimes with technology. As such, routine activity theory has important implications for understanding crimes committed with or prevented with computers, other electronic IT devices, or information systems. The theory closely relates to choices made by cyber-criminals when deciding which targets to strike regarding possibilities of being investigated, prosecuted, and punished (McQuade, 2006).

Social Learning Theory

Essentially, social learning theory posits that cybercriminals abuse and commit cybercrimes using computers and other forms of IT because they learn how to do so from others (McQuade, 2006). The four key concepts that are central to the social learning theory are: differential association, definitions, imitations, and differential reinforcement. Differential association relates to the individual involvement in deviant behaviour because of social interactions with deviant others. Definitions are beliefs, attitudes, justifications, or orientations which the individual uses to designate certain behaviour as either good or bad. The involvement or non-involvement of individuals in delinquent behaviour such as cybercrime is determined by their designation of definitions as either deviant or non-deviant including other stimuli present in a particular situation. Imitation or modelling is a process of learning behaviour through socialisation. Deviant peers may provide examples and share knowledge, attitude, beliefs, and techniques with an individual to influence his/her participation in deviant conduct such as cybercrime. Deferential reinforcement/ punishment involves the balance between the anticipated and real consequences of engaging in certain type of behaviours such as cyber-fraud. The balance of rewards and punishment determine whether an individual will offend or not.

Cyber-offending in Nigeria: A synopsis

According to Tade & Aliu (as cited in Ibrahim, 2016), most young people in Nigeria involved in cybercrime are involved in general are involved in cyber fraud in general. According to Ibrahim, 2016), perpetrators of cybercrime in Nigeria have over the years been persistently implicated in money-oriented than psychosocial and geopolitical cybercrime. A number of studies (Chawki. Et al. 2015; Ellis, 2016) reinforce the broader narrative that perpetrators of cybercrime in Nigeria focus basically on cyber-fraud. Longe et al. (as cited in Ibrahim, 2016) asserted that the Nigerian 419 fraud birthed and revolutionised by Nigerian fraudsters such as Mr Fred Ajiduah is strongly rooted in socioeconomics. In other words, Ibrahim (2016) validly noted that cyber-offending in Nigeria can be conceptualised simply as the use of computer/internet to commit fraud. The table below also reinforces the narrative that cyber-offending in Nigeria is deeply rooted in socioeconomics and can be conceptualised largely as involvement in cyber-fraud.

Some selected cases of Cyber-Offending in Nigeria

S/N	Date	Narrative	State
1	14-09-2022	Justice M. Itsueli of Edo State High Court, sitting in Benin city convicted and sentenced 2 persons to two years imprisonment for cybercrime.	Edo state
2	12-09-2022	Justice Nasiru U. Sadiq of the Kaduna State High Court, sitting in Kaduna, convicted and sentenced two internet fraudsters to five years, six months imprisonment for internet related offences and cheating.	Kaduna
3	08-09-2022	Justice Adebayo Yusuf of the Kwara State High Court, Ilorin and Muhammed Sani of the Federal High Court in Ilorin convicted 2 siblings on two count-charges bordering on cybercrime (retention of proceeds of unlawful activities)	Kwara
4	09-09-2022	Justice M. Itsueli of Edo State High court, sitting in Benin city, convicted and sentenced a duo to eight years imprisonment internet-related fraud. Explicitly, they were convicted one count separate charge, bordering on retention of proceeds of criminal conduct and possession of documents containing and false pretence.	Edo
5	07-09-2022	Justice Nasiru U. Sadiq of the Kaduna State High Court convicted and sentenced four internet fraudsters to various terms of imprisonment for internet related offences and impersonation. Explicitly, they were convicted on one-count separate charge bordering on internet fraud upon their arraignment by the Kaduna Zonal Command of Economic and Financial Crimes Commission.	Kaduna
6	31-08-2022	Justice Nasiru U. Sadiq of the Kaduna High Court convicted and sentenced eight internet fraudsters to various terms of imprisonment for internet-related offences, cheating and impersonation.	Kaduna
7	01-09-2022	Justice M. Itsueli of Edo State High Court convicted and sentenced one person to two years imprisonment on one-count charge bordering on cyber-fraud.	Edo
8	29-08-2022	Justice M.Itsueli of the Edo State High Court in Benin city, Edo state convicted and sentenced three internet fraudsters to nine years imprisonment on one-count separate charge bordering on possession of documents containing false pretence and retention of illegal proceeds of crime.	Edo
9	29-08-2022	Justice Ibrahim Yusuf of Kwara State High Court, Ilorin, Kwara state convicted and sentenced five persons on three-count separate charges bordering on internet fraud, cheating and possession of fraudulent funds.	Kwara
10	29-03-2022	Justice M.S. Shuaibu of the Federal High Court in Benin city, Edo State convicted and sentenced a woman to five years imprisonment on one-count charge for aiding her son who is an alleged fraudster. The woman was found guilty of receiving N91,296,150 "being proceeds of her son's criminal activities".	Edo
11	26-09-2022	Justices A.A. Bello and Darius Khobo of Kaduna State High Court convicted and sentenced five internet fraudsters to different terms of imprisonment for one-count separate charge bordering on internet fraud.	Kaduna
12	26-09-2022	Justice Muhammed Sani of the Federal High Court in Ilorin convicted and sentenced five internet fraudsters to terms of imprisonment bordering on cybercrime and possession of fraudulent funds.	Kwara
13	27-09-2022	Justices EfeIkponwasa and M. Itsueli of Edo State High Court convicted and sentenced eight (8) internet fraudsters to sixteen (16) years imprisonment.	Edo
14	27-09-2022	An Oyo State High Court sitting in Ibadan convicted and sentenced sixty-six (66) in internet fraudsters to various jail terms, ranging from two weeks, four months, of community service and to ten months imprisonment.	Oyo

Source: EFCC (2022)

Conclusion and Recommendations

Cybercrime is a serious problem ravaging the contemporary world. Crime setting has significantly moved from terrestrial realm to the cyberspace. Traditional crimes have over the years revolved into cybercrimes such as cyber-fraud, cyber-theft to mention but a few. There is no gain saying the fact that billions of dollars have been lost to cybercrimes as much as billions of dollars have been expended on cyber-security globally. The cost of cybercrime globally leaves much to be desired. In response to this, nation-states have enacted legislations unilaterally, bi-laterally and multi-laterally to combat the menace. Even at this, the menace of cybercrime still rears its ugly head.

In Nigeria, unlike the developed countries such as United States, there is a paucity/dearthof empirical studies around cyber offending from a correction's perspective i.e., seeking empirical insight from correctional centres and examining the characteristics of offenders. A proper understanding of the behavioural pattern, background, and characteristics of offenders of cyber-crime will come in handy in policy formulation and enactment of legislations that will better tackle the problem of cybercrime in Nigeria. By way of recommendation, the Nigerian state should address the issue of poverty, cumulative deprivation and ensure the proper implementation of the Cyber Crime Act of 2015.

References

Adesina, O. (2017). Cybercrime and Poverty in Nigeria. *Canada Social Science*, 13(4): 19-29

African Cyber Security (2019) *2019 Global Threat Report: Adversary tradecraft and the importance of speed.* African Cyber Security

Bossler, A &Berenblum, T. (2019). Introduction: New direction in Cyber Research. *Journal of Crime and Justice, 42(5):495-499*

Daultrey, S. (2017). Cybercrime: Invisible Problems, Imperfect Solutions. Online.

Davos (2019) The World Economic Forum-Globalization 4.0. Retrieved on August 1, 2021 from https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/

Hadzhidimova, L. & Payne, B. (2019). "The Profile of the International Offender in the U.S. *International journal of Cyber security, Intelligence and Cybercrime*, 2(1)40-55.

Harbinson, E. & Selzer, N (2019). The Risk and Needs of Cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice* 42(5): 582-598

Holt, T. & Bossler, A(2016).*Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Crime Sciences Series. New York: Routledge.

Holt, T., Bossler, A &Seigfried-Spellar, K.(2018). *Cybercrime and Digital Forensics: An Introduction*. 2nd ed. New York: Routledge

Ibrahim, S. (2016). Social and Contextual Taxonomy of Cybercrime: Socio-economic Theory of Nigerian Cyber criminals. *Journal of Law, crime and Justice*,47: 44-57

Internet Crime Compliant Centre (IC3) (2021). 2020 Internet Crime Report. Retrieved August 1, 2021 from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Internet World Stats (2021). Internet Usage and World Population Statistics Estimates. Retrieved August 1, 2021 from https://www.internetworldstats.com/stats.htm

Jaishankar, K. (2008). Space Transition Theory of cybercrime. In F. Schmallager& M. Pittaro (Eds.)Crimes of the Internet (pp 283-301), Prentice Hall.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2):77-81

Kranenbarg, M., Laan, A., Poot, C., Verhoeven, M., Wagen, W. &Weijters, G. (2017). Individual Cybercrime Offenders. In E.R. Leukfeldt (Ed.), *Research Agenda: The Human Factor in Cybercrime and*

Cybersecurity. Den Haag: Eleven International Publishing

Kranenbarg, M., Busler, S., Van Gelder, J and Bernasio, W (2018). Cyber Offending and Traditional Offending over the Life-Course: An Empirical Comparison. *Journal of Development Life Course Criminology, 4(1): 343-384.*

Lau, L. (2018). Cybercrime 'Pandemic' may have cost the world $600 billion last year. Retrieved August 1 from https://www.cnbc.com/2018/02/22/cybercrime-pandemic- may-have-cost-the-world-600-billion-last-year.html

McQuade, S. (2006). Understanding and Managing Cybercrime (1st Ed), Pearson.

Ndubueze, P. (2020). *Cybercrime and Legislation in an African Context*. In T.J. Holt & A.M. Bossler (Eds.) The Palgrave handbook of International Cybercrime.

Signe, L. & Signe, K. (2018). *"Global Cybercrimes and Weak Cyber security threaten businesses in Africa*. Online.

Umaru, I. (2019). The Impact of Cybercrime on the Nigerian Economy and Banking System. *National Deposit Insurance Company (NDIC) Quarterly 34(12):1-20.*

United Nations Population Fund (UNDF) (2021). World Population Data. Retrieved on August 1, 2021 from https://www.unfpa.org/data/world-population-dashboard.

UNODC (2013). *Comprehensive Study on Cybercrime*. United Nations.